Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	500.38991X00
First Inventor or Application Identifier	Daisuke SHINOHARA
Title	See 1 in Addendum
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] * Fee Transmittal Form *(e.g., PTO/SB/17)* *(Submit an original and a duplicate for fee processing)*
2. [X] Specification [Total Pages 26]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings *(if filed)*
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. [X] Drawing(s) *(35 U.S.C. 113)* [Total Sheets 6]
4. Oath or Declaration [Total Pages]
   a. [ ] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
      i. [ ] DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

** NOTE FOR ITEMS 1 & 13 IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

5. [ ] Microfiche Computer Program *(Appendix)*
6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [ ] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement [ ] Power of Attorney *(when there is an assignee)*
9. [ ] English Translation Document *(if applicable)*
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. [ ] * Small Entity Statement(s) *(PTO/SB/09-12)* [ ] Statement filed in prior application Status still proper and desired
14. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. [X] Other: Figs. 1-8; Credit Card Payment Form; List

16. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____

Prior application information: Examiner _____ Group / Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[X] *Customer Number or Bar Code Label* 020457 *(Insert Customer No. or Attach bar code label here)* or [ ] *Correspondence address below*

Name					
Address					
City		State		Zip Code	
Country		Telephone		Fax	

Name (Print/Type)	Carl I. Brundidge	Registration No. (Attorney/Agent)	29,621
Signature		Date	9-6-00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Attachment to PTO/SB/05 (4/98) Utility Patent Application Transmittal

1. A REMOTE MAINTENANCE METHOD OF AN INFORMATION PROCESSING APPARATUS

PTO/SB/17 (12/99)
Approved for use through 09/30/2000 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.
Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB/09-12. See 37 C.F.R. §§ 1.27 and 1.28

TOTAL AMOUNT OF PAYMENT ($) 690.00

Complete if Known	
Application Number	
Filing Date	September 6, 2000
First Named Inventor	Daisuke SHINOHARA
Examiner Name	
Group / Art Unit	
Attorney Docket No.	500.38991X00

METHOD OF PAYMENT (check one)

1. ☐ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 01-2135

Deposit Account Name: Antonelli,Terry,Stout&Kraus,LLP

☒ Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

2. ☒ **Payment Enclosed:** ☐ Check ☐ Money Order ☒ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility filing fee	690.00
106	310	206	155	Design filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 690.00

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below		Fee Paid
Total Claims	10	-20** = 0	x 18	=	0
Independent Claims	1	- 3** = 0	x 78	=	0
Multiple Dependent					0

***or number previously paid, if greater; For Reissues, see below*

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim, if not paid
109	78	209	39	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	0.00
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	0.00
139	130	139	130	Non-English specification	0.00
147	2,520	147	2,520	For filing a request for reexamination	0.00
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	0.00
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	0.00
115	110	215	55	Extension for reply within first month	0.00
116	380	216	190	Extension for reply within second month	0.00
117	870	217	435	Extension for reply within third month	0.00
118	1,360	218	680	Extension for reply within fourth month	0.00
128	1,850	228	925	Extension for reply within fifth month	0.00
119	300	219	150	Notice of Appeal	0.00
120	300	220	150	Filing a brief in support of an appeal	0.00
121	260	221	130	Request for oral hearing	0.00
138	1,510	138	1,510	Petition to institute a public use proceeding	0.00
140	110	240	55	Petition to revive - unavoidable	0.00
141	1,210	241	605	Petition to revive - unintentional	0.00
142	1,210	242	605	Utility issue fee (or reissue)	0.00
143	430	243	215	Design issue fee	0.00
144	580	244	290	Plant issue fee	0.00
122	130	122	130	Petitions to the Commissioner	0.00
123	50	123	50	Petitions related to provisional applications	0.00
126	240	126	240	Submission of Information Disclosure Stmt	0.00
581	40	581	40	Recording each patent assignment per property (times number of properties)	0.00
146	690	246	345	Filing a submission after final rejection (37 CFR § 1.129(a))	0.00
149	690	249	345	For each additional invention to be examined (37 CFR § 1.129(b))	0.00
Other fee (specify)					0.00
Other fee (specify)					0.00

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Carl J. Brundidge	Registration No. (Attorney/Agent)	29,621	Telephone	703-312-6600
Signature				Date	9-06-00

WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

A REMOTE MAINTENANCE METHOD OF AN INFORMATION PROCESSING APPARATUS

BACKGROUND OF THE INVENTION

The present invention relates to a method for maintaining an information processing apparatus from a remote place, and more particularly to a method for performing maintenance by switching a program which is loaded upon start-up of an information processing apparatus to a maintenance program which is held in a server on a network as requested by an operator at a remote place.

The maintenance program must be run on the information processing apparatus without operating an operating system. Therefore, the information processing apparatus requiring the execution of the maintenance program is generally maintained by booting the system from removable media such as a floppy disk and running the maintenance program stored on the removable media by a maintenance person on the spot.

An example of the remote maintenance is disclosed in JP-A-10-214183 which relates to a technology to update firmware on the information processing apparatus from a remote place. According to the above disclosed technology, the information processing apparatus is designed to always get a boot program from a remote boot process on a network so to realize the remote update of firmware on the information processing

apparatus.

Specifically, when the information processing apparatus is booted, the remote boot process compares a version of the firmware stored in the information processing apparatus with a version of the latest firmware. If the version of firmware of the information processing apparatus is old, the remote boot process automatically sends a firmware update program. If the information processing apparatus has the latest version of firmware, the remote boot process sends a boot program for normal operations to the information processing apparatus.

By configuring as described above, JP-A-10-214183 can update the firmware of the information processing apparatus to the latest version upon a system reset of the subject information processing apparatus after preparing new firmware for a server.

SUMMARY OF THE INVENTION

When a maintenance person goes to the actual place and executes a maintenance program in a conventional way, it takes a lot of time from the occurrence of an actual request to the completion of execution of the maintenance program. There is also a problem that the amount of work of the maintenance person increases proportionally with an increase in number of machines to be maintained.

When firmware is updated according to the

aforesaid prior art, it is necessary to perform the system reset on the side of the information processing apparatus, and there is a disadvantage that the firmware cannot be updated by controlling from a remote place.

It is a main object of the present invention to remedy the aforesaid problems of the prior art and to make it possible to execute a maintenance program of the information processing apparatus by remotely controlling when it is necessary to execute the maintenance program.

To achieve the aforesaid object, the present invention executes the maintenance program on the information processing apparatus by controlling from a remote management subsystem in a computer system which comprises the remote management subsystem and an information processing apparatus provided with a communications device for communications through a network.

In a preferred embodiment of the present invention, it is instructed from the remote management subsystem to the information processing apparatus to set the communications device as a boot device for obtaining a program when the information processing apparatus is booted in order to execute the maintenance program. According to the instruction, the information processing apparatus sets the communications device as the boot device. Then, the remote management subsystem instructs the information processing apparatus to perform a system reset. According to the instruction about the system

reset, an agent operating on the information processing apparatus resets the information processing apparatus. When the information processing apparatus is reset, the communications device is set as the boot device, and a program to be executed is requested to the remote management subsystem. According to the request from the information processing apparatus, the remote management subsystem transfers the maintenance program to the information processing apparatus, and the maintenance program is used to boot the information processing apparatus and started to be executed.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic system structure diagram showing connected relationships of equipment configuring the system according to a first embodiment of the present invention;

Fig. 2 is a simplified block diagram showing the structure of a management console;

Fig. 3 is a simplified block diagram showing the structure of a remote management server;

Fig. 4 is a simplified block diagram showing the structure of an information processing apparatus;

Fig. 5 is a sequence diagram showing a flow of processing performed between a management console 10 and a remote management server 20 when firmware is remotely updated;

Fig. 6 is a timing chart showing a flow of

processing by a remote management server to an information processing apparatus to set a communications device as a boot device when firmware is remotely updated;

Fig. 7 is a timing chart showing a flow of processing performed after a system reset of the information processing apparatus is performed; and

Fig. 8 is a schematic system structure diagram showing connected relationships of equipment configuring the system according to a second embodiment of the present invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

Fig. 1 is a schematic system structure diagram showing connected relationships of equipment configuring the system according to a first embodiment of the present invention.

A management console 10 of this embodiment is connected to a remote management server 20 through a communications channel 70. The remote management server 20 is connected to an information processing apparatus 40 through a communications channel 71. A remote management subsystem comprises the management console 10 and the remote management server 20, and the information processing apparatus 40 is maintained under the control of the remote management subsystem.

The system of this embodiment makes it possible to update firmware of the information

processing apparatus 40 as one way of remote maintenance. The firmware of the information processing apparatus 40 of this embodiment is updated by the information processing apparatus 40 which obtains a firmware update program as the maintenance program from the remote management server 20 installed in a distant place.

The management console 10 is a terminal which achieves the function of a remote management console 11 which provides a user interface for an operator. The remote management server 20 includes a remote management process 21 for sending a request from the remote management console 11 to the information processing apparatus 40 and a remote boot process 28 for providing the information processing apparatus 40 with a firmware update program 30. The information processing apparatus 40 includes a nonvolatile memory 56 which stores boot device information 57, a management agent 41 which rewrites the content of the boot device information 57 within the nonvolatile memory 56, a communications device 58 which is provided with a remote boot section 61 for obtaining the firmware update program 30 from the remote management server 20 and a service processor 53 which is provided with a power control section 55 for controlling on/off of the power supply of the main body according to a request from the remote management server 20.

Fig. 2 is a simplified block diagram showing

the structure of the management console 10.

The console device 10 can be a computer such as a so-called personal computer (PC) or a workstation (WS). The console device 10 has the remote management console 11 which is a program run on the console device 10 and provides a console function operated by the operator in charge of the remote maintenance.

The remote management console 11 has an information processing apparatus management section 12, a firmware information acquisition section 13 and a firmware update execution section 14 as function processing sections related to the present invention.

The information processing apparatus management section 12 shows a list of information processing apparatuses 40 to be managed on a screen so to assist the operator to decide which information processing apparatus 40 has the firmware updated. The firmware information acquisition section 13 shows a list of firmware mounted on the subject information processing apparatuses 40 and respective versions of firmware which can be updated. Thus, it assists the operator in deciding which version of firmware is updated. The firmware update execution section 14 sends a request for updating to the decided version of firmware to the remote management server 20 and then monitors the progress of update of the firmware on the information processing apparatus 40, thereby assisting the operator to detect success or failure of the update.

Fig. 3 is a simplified block diagram showing a logical structure of the remote management server 20.

Specifically, a computer such as PC or WS is used as the remote management server 20. The remote management server 20 has the remote management process 21, and a remote boot process 28 as programs which are run thereon. The remote management server 20 has a certification file 31, which is used to certify the firmware update program 30, in an unshown disk.

The remote management process 21 has a firmware information acquisition section 22, a communications device identification information acquisition section 24, a remote boot process detection section 25, a boot device setting section 26 and a remote power control section 27.

The firmware information acquisition section 22 obtains information about the version of firmware from the information processing apparatus 40 to be maintained. The firmware information acquisition section 22 refers to firmware management information 23 to obtain a list of versions of firmware which can be updated and sends the list to the management console 10. The firmware management information 23 is information for managing types and versions of firmware, versions which can be updated, and file names of corresponding firmware update programs. The firmware information acquisition section 22 obtains the information on the version of the updating firmware which is designated by

the operator through the management console 10 and passes the obtained information to the remote boot process 28.

The communications device identification information acquisition section 24 obtains communications device identification information from the information processing apparatus 40 to be maintained and passes it to the remote boot process 28.

The communications device identification information is identification information which is uniquely decided by the information processing apparatus. As the communications device identification information, MAC (Media Access Control) address is used in this embodiment.

The remote boot process detection section 25 sends an acquisition request for a pseudo firmware update program to all machines on the network and checks the reception or not of a reply. When there is a reply to the acquisition request for the pseudo firmware update program, it means that there is a machine, which replies to the firmware update program acquisition request sent by the information processing apparatus 40, other than the remote management server 20. Then, the remote boot process detection section 25 sends an error to the management console 10.

When firmware is to be updated, the boot device setting section 26 sets the boot device of the subject information processing apparatus 40 as a

communications device.

After the execution of firmware update program 30 is completed, the remote power control section 27 controls to turn on/off the power of the subject information processing apparatus 40.

The remote boot process 28 receives the version information of the update firmware from the remote management process 21 and the communications device identification information of the information processing apparatus 40 as parameters and registers the communications device identification information into the communications device registration information 29 which manages a list of information processing apparatuses 40 which are subjected to the update of firmware. Then, the remote boot process 28 sends the designated version of firmware update program 30 according to the acquisition request from the subject information processing apparatus 40. The remote boot process 28 sends the certification file 31 corresponding to the firmware update program 30 in response to the request from the information processing apparatus 40.

Fig. 4 is a simplified block diagram showing a structure of the information processing apparatus 40.

The information processing apparatus 40 is a computer such as PC or WS which executes an application program or the like for performing various types of transaction processing. The information processing apparatus 40 comprises hardware 52, firmware 49

necessary for operating the hardware 52, an operating system 45 which runs on the hardware and controls the execution of application programs or the like.

The management agent 41 comprises a firmware information acquisition section 42, a boot device setting section 43 and a communications device identification information acquisition section 44. The management agent 41 can invoke an I/O routine of firmware through the operating system 45 in an environment where the operating system 45 is operating to update the boot device information.

The firmware information acquisition section 42 obtains version information 50 of the body firmware 49 according to the request by the remote management server 20.

The boot device setting section 43 sets to obtain the boot program from the communications device 58 at the time of booting after the system reset according to the request by the remote management server 20.

The communications device identification information acquisition section 44 obtains identification information (MAC address) which is allocated to the communications device 58 and sends it to the remote management server.

The operating system 45 has a firmware information acquisition driver 46, a boot device setting driver 47 and a communications device driver 48 in order

to achieve the firmware updating function. These drivers are configured as part of the operating system 45 or as a program module which is activated by the operating system 45 when executed.

The firmware information acquisition driver 46 obtains the version information 50 from the firmware 49 in which it is stored. The boot device setting driver 47 invokes an I/O routine 51 which is on the firmware 49 and rewrites the boot device information 57 which is stored in the nonvolatile memory 56.

The communications device driver 48 accesses the communications device 58 through an unshown bus to obtain communications device identification information 59.

The hardware 52 has the service processor 53, the nonvolatile memory 56 and the communications device 58 to realize the firmware update function.

The service processor 53 comprises a communications processing section 54 and the power control section 55 which controls on/off of the power of the information processing apparatus 40. The power supplied to the service processor 53 is separately controlled from the one supplied to the information processing apparatus 40.

The boot device information 57 which describes the order of devices obtaining the boot program at booting is stored in the nonvolatile memory 56. The boot device information 57 is set by the I/O routine 51

on the firmware 49.

The MAC address, which is used as the communications device identification information 59 in this embodiment, is uniquely allocated to the communications device 58. The communications device 58 has a communications processing section 60 which communicates with other machines on the network, the remote boot section 61 which obtains and executes the boot program from a machine on the network and a file certification section 62 which obtains a certification file corresponding to the boot program and checks the presence or not of a difference between the original boot program and the obtained boot program.

Fig. 5 is a sequence diagram showing a flow of processing performed between the management console 10 and the remote management server 20 when the firmware is remotely updated.

The management console 10 requests the remote management server 20 to obtain the list of information processing apparatuses. In response to the request, the remote management server 20 obtains the list of information processing apparatuses from the firmware management information 23 and sends it to the management console 10.

The management console 10 shows the list of information processing apparatuses received from the remote management server on a display. The operator decides the information processing apparatus 40, whose

firmware is updated, from the list shown on the display and operates the management console 10 to specify the information processing apparatus 40. When the information processing apparatus whose firmware is updated is decided by the operator, the console device 10 sends the information acquisition request for the firmware stored in the information processing apparatus 40 to the remote management server 20.

In response to the information acquisition request, the remote management server 20 obtains types of firmware and versions from the information processing apparatus 40 on which they are mounted. Then, the remote management server 20 refers to the data stored in the firmware management information 23 and decides a version of firmware which can be updated. The remote management server 20 sends information about the decided version of firmware, which can be updated, to the management console.

The list of firmware stored in the information processing apparatus 40 and decided by the operator, the respective versions of firmware and the versions of firmware which can be updated are shown on the screen of the management console 10. The operator decides the version of firmware to be updated and enters it into the management console 10.

After the version of software to be updated is decided by the operator, the management console 10 sends an update execution request to the remote management

server 20. In response to the request, the remote management server 20 starts update processing of the firmware.

Fig. 6 is a timing chart showing a flow of processing by the remote management server 20 to the information processing apparatus 40 to set the communications device 58 as the boot device when the firmware is remotely updated.

In the above processing, the remote management server 20 requests the information processing apparatus 40 for the communications device identification information 59 in the communications device 58 mounted on the information processing apparatus 40. In response to the request, the information processing apparatus obtains the communications device identification information 59 which is set in the communications device 58 and sends it to the remote management server 20.

The remote management server 20 sends the acquisition request for a pseudo firmware update program including the acquired communications device identification information 59 to all machines on the network and checks the presence or not of a reply to the acquisition request.

When there is a reply from the network in response to the acquisition request, it means that there are other machines on the network responding to the request when the information processing apparatus 40 sends the firmware update program acquisition request.

In such a case, the remote management server 20 sends an error to the management console.

When there is no reply from the network to the acquisition request, the remote management server 20 registers the obtained communications device identification information 59 into the communications information registration information 29. Then, the remote management server 20 requests the information processing apparatus 40 to set the communications device 58 as the boot device.

Upon receiving the request for setting the boot device from the remote management server 20, the information processing apparatus 40 uses the I/O routine 51 of the firmware 49 to rewrite the boot device information 57 within the nonvolatile memory 56 and sets the communications device 58 as the boot device.

After setting the communications device 58 as the boot device, the information processing apparatus 40 performs a system reset of the information processing apparatus 40 itself.

Fig. 7 is a timing chart showing a flow of processing performed after the system reset of the information processing apparatus 40 is made.

After the system reset, the boot processing is started with the communications device 58 used as the boot device, and the information processing apparatus 40 sends a firmware update program acquisition request including the communications device identification

information 59 to all the machines on the network.

Upon receiving the firmware update program acquisition request, the remote management server 20 checks whether the communications device identification information included in the received acquisition request is registered in the communications device registration information 29. When the pertinent communications device identification information is registered, the firmware update program 30 is sent to the sending side, the information processing apparatus 40.

After receiving the firmware update program 30, the information processing apparatus 40 requests the remote management server 20 to send the certification file 31. After receiving the certification file 31 from the remote management server 20, the information processing apparatus 40 certifies whether the firmware update program 30 acquired in the file certification section 62 is identical with the original firmware update program. When it is found that the acquired firmware update program 30 is identical with the original program, the information processing apparatus 40 starts to execute the newly obtained firmware update program 30 to update the firmware.

After the execution of the firmware update program 30 is completed, the information processing apparatus 40 sets the boot device as a local storage device and sends a notice of execution completion of the firmware update program to the remote management server

20.

When the remote management server 20 receives the notice of execution completion of the firmware update program, it controls the power of the information processing apparatus 40 by the remote power control section 27 to turn off the power of the information processing apparatus 40. The remote power control section 27 turns on again the power of the information processing apparatus 40 after a lapse of predetermined time. Thus, the information processing apparatus 40 performs the boot processing from the local storage device and loads the operating system according to the ordinary procedure to enable the execution of various types of applications. Thus, the firmware update processing is completed.

Fig. 8 is a system structure diagram showing a schematic structure of the system according to another embodiment of the present invention.

This embodiment describes briefly a system for executing as the maintenance program a diagnosis program for diagnosing the information processing apparatus by sending the diagnosis program from a remote place to the information processing apparatus.

The system of this embodiment is also configured in the same way as the system shown in Fig. 1 and has the management console 10, the remote management server 20 and the information processing apparatus 40. The system of this embodiment does not need the control

of on/off of the power of the information processing apparatus 40 before and after the execution of the diagnosis program which is used as the maintenance program. Therefore, this embodiment is different from the first embodiment and does not especially need to install a service processor in the information processing apparatus 40.

In this embodiment, the information processing apparatus 40 sets the communications device as the boot device according to the instruction from the management console 10, performs the system reset of the information processing apparatus according to the control from the remote management server 20 and loads the diagnosis program 80 from the remote management server 20 into the information processing apparatus 40 to execute it. After the execution of the diagnosis program is completed, the boot device of the information processing apparatus 40 is set to a local storage device under the control of the remote management server 20. Then, the system reset is performed again under the control of the remote management server 20 to return to the ordinary processing, and the diagnosis processing is terminated.

According to the embodiments described above, the boot device of the information processing apparatus such as PC can be switched according to the control from the remote management server connected with it through the network, and the information processing apparatus can be booted from the maintenance program by remote

operation. And, the power on/off of the information processing apparatus can be controlled from the remote management server as required, and the maintenance of firmware which requires the power control when it is updated can be performed remotely.

It is to be understood that the present invention is not limited to the embodiments described above and can be modified into various embodiments without departing from the spirit and the scope of the invention. For example, the management console and the remote management server each are independent apparatuses mutually connected through the network in the aforesaid embodiments but may be configured of a single computer.

As described above, when it is necessary to execute the maintenance program according to the present invention, the maintenance program of the information processing apparatus can be executed from a remote place.

WHAT IS CLAIMED IS:

1. A maintenance method, for use in a computer system having a remote management subsystem and an information processing apparatus provided with a communications device for communicating with said management subsystem, for maintaining said information processing apparatus, comprising the steps of:

instructing from said remote management subsystem to said information processing apparatus to set said communications device as a boot device to obtain a program when said information processing apparatus is booted;

setting said communications device as the boot device by said information processing apparatus according to said instruction;

instructing a system reset from said remote management subsystem to said information processing apparatus;

resetting said information processing apparatus according to the system reset instruction; and

starting the execution of a maintenance program by acquiring said maintenance program from said remote management subsystem by said information processing apparatus with said communications device used as the boot device to boot the system.

2. A maintenance method according to claim 1, wherein said maintenance program acquired from said remote management subsystem in said execution starting

step is a program for updating firmware possessed by said information processing apparatus.

3. A maintenance method according to claim 2, further comprising a step of controlling on/off of the power of said information processing apparatus according to an instruction from said remote management subsystem after the execution of the maintenance program is completed.

4. A maintenance method according to claim 2, further comprising the steps of:

acquiring information about the firmware from said information processing apparatus, which has the information about the firmware, by said remote management subsystem; and

judging a program to be sent to said information processing apparatus according to the information about the firmware.

5. A maintenance method according to claim 1, wherein said execution starting step includes a step to check that the obtained maintenance program is an appropriate program.

6. A maintenance method according to claim 5, wherein said checking step includes a step of obtaining a certification file corresponding to said maintenance program from said remote management subsystem and a step of inspecting said maintenance program according to said certification file.

7. A maintenance method according to claim 1,

further comprising the steps of:

acquiring identification information, which is used to obtain said maintenance program by said information processing apparatus, by said remote management subsystem;

sending a request to obtain a pseudo maintenance program by said identification information; and

checking the presence or not of a reply to the request to obtain the pseudo maintenance program.

8. A maintenance method according to claim 1, further comprising the steps of:

registering previously identification information of an information processing apparatus subjected to maintenance into said remote management subsystem;

receiving input of identification information for specifying said information processing apparatus prior to the instruction to set said boot device; and

judging whether the received identification information is included in the registered identification information.

9. A maintenance method according to claim 1, wherein the setting of said boot device and said reset are performed by a management agent which operates on said information processing apparatus.

10. A maintenance method according to claim 9, wherein said boot device is set by said management agent

which calls an I/O routine of the firmware in an environment where an operating system of said information processing apparatus is operating.

ABSTRACT OF THE DISCLOSURE

A maintenance method, for use in a computer system which includes a remote management subsystem and an information processing apparatus provided with a communications device for communicating through a network, for executing a maintenance program on the information processing apparatus under the control of the remote management subsystem is disclosed. For execution of the maintenance program, the remote management subsystem gives an instruction to the information processing apparatus to set the communications device as a boot device to obtain a program when the information processing apparatus is booted. According to the instruction, the information processing apparatus sets the communications device as the boot device. The remote management subsystem gives an instruction for a system reset to the information processing apparatus. In response to the instruction for the system reset, an agent operating on the information processing apparatus resets the information processing apparatus. When the information processing apparatus is reset, it requires a program to be executed to the remote management subsystem with the communications device used as the boot device. According to the requirement from the information processing apparatus, the remote management subsystem transfers the maintenance program to the information processing apparatus. This maintenance program is used to boot the

information processing apparatus and started to be executed.

FIG. 1

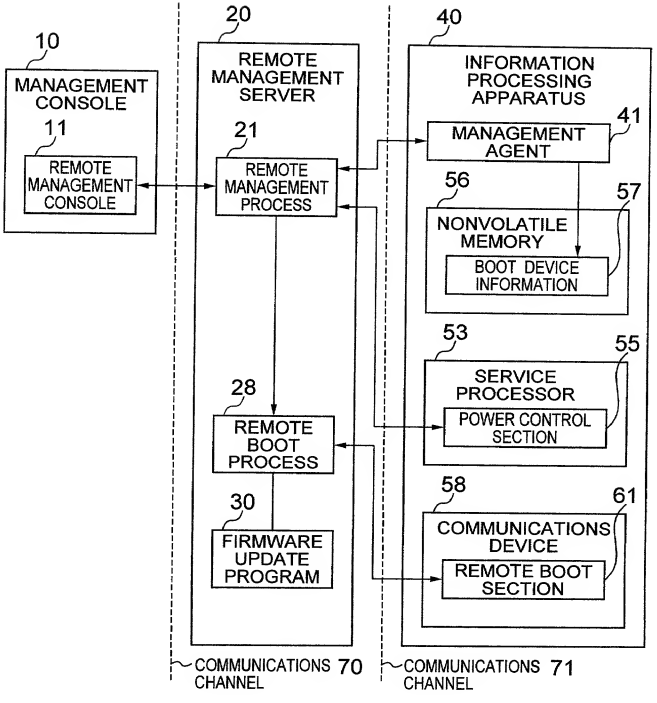

10
MANAGEMENT CONSOLE
11
REMOTE MANAGEMENT CONSOLE
20
REMOTE MANAGEMENT SERVER
21
REMOTE MANAGEMENT PROCESS
28
REMOTE BOOT PROCESS
30
FIRMWARE UPDATE PROGRAM
40
INFORMATION PROCESSING APPARATUS
41
MANAGEMENT AGENT
56
NONVOLATILE MEMORY
57
BOOT DEVICE INFORMATION
53
SERVICE PROCESSOR
55
POWER CONTROL SECTION
58
COMMUNICATIONS DEVICE
61
REMOTE BOOT SECTION
COMMUNICATIONS CHANNEL 70
COMMUNICATIONS CHANNEL 71

FIG. 2

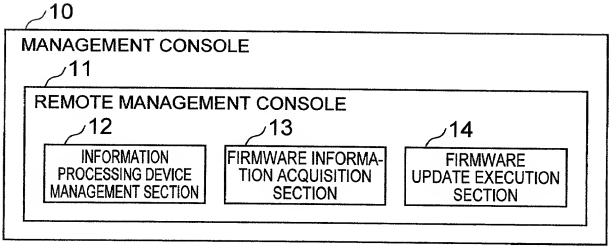

10
MANAGEMENT CONSOLE
11
REMOTE MANAGEMENT CONSOLE
12
INFORMATION PROCESSING DEVICE MANAGEMENT SECTION
13
FIRMWARE INFORMATION ACQUISITION SECTION
14
FIRMWARE UPDATE EXECUTION SECTION

FIG. 3

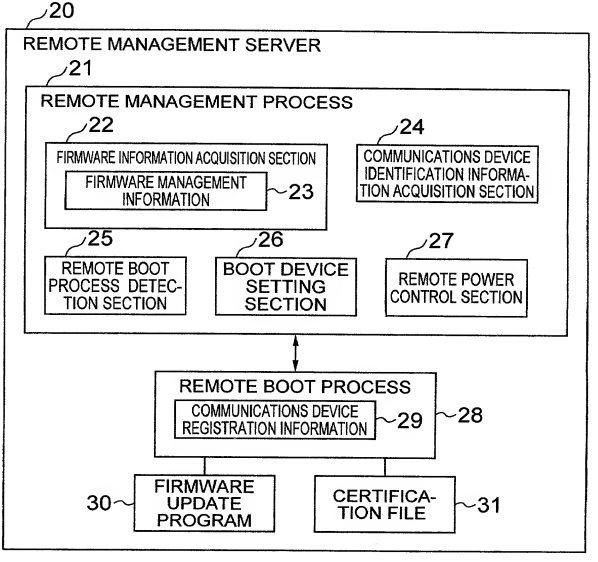

20
REMOTE MANAGEMENT SERVER
21
REMOTE MANAGEMENT PROCESS
22
FIRMWARE INFORMATION ACQUISITION SECTION
FIRMWARE MANAGEMENT INFORMATION
23
24
COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION ACQUISITION SECTION
25
REMOTE BOOT PROCESS DETECTION SECTION
26
BOOT DEVICE SETTING SECTION
27
REMOTE POWER CONTROL SECTION
REMOTE BOOT PROCESS
COMMUNICATIONS DEVICE REGISTRATION INFORMATION
29
28
30
FIRMWARE UPDATE PROGRAM
CERTIFICATION FILE
31

FIG. 4

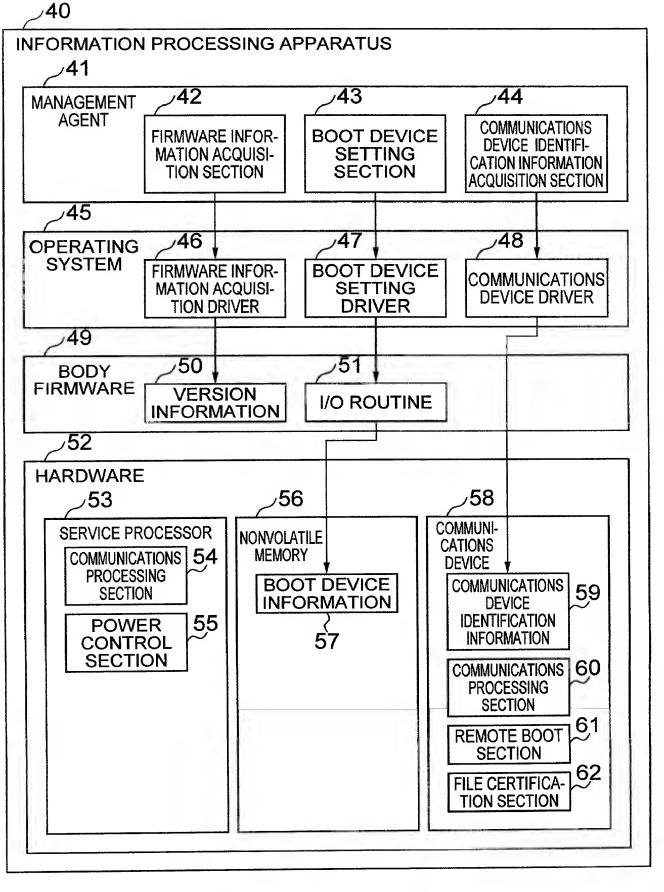

40
INFORMATION PROCESSING APPARATUS
41
MANAGEMENT AGENT
42
FIRMWARE INFORMATION ACQUISITION SECTION
43
BOOT DEVICE SETTING SECTION
44
COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION ACQUISITION SECTION
45
OPERATING SYSTEM
46
FIRMWARE INFORMATION ACQUISITION DRIVER
47
BOOT DEVICE SETTING DRIVER
48
COMMUNICATIONS DEVICE DRIVER
49
BODY FIRMWARE
50
VERSION INFORMATION
51
I/O ROUTINE
52
HARDWARE
53
SERVICE PROCESSOR
COMMUNICATIONS PROCESSING SECTION
54
POWER CONTROL SECTION
55
56
NONVOLATILE MEMORY
BOOT DEVICE INFORMATION
57
58
COMMUNICATIONS DEVICE
COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION
59
COMMUNICATIONS PROCESSING SECTION
60
REMOTE BOOT SECTION
61
FILE CERTIFICATION SECTION
62

FIG. 5

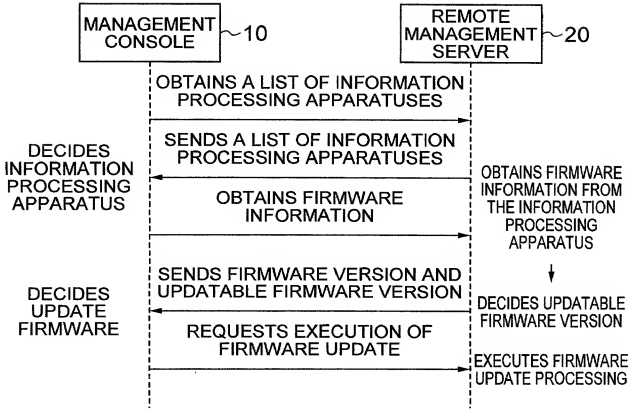

MANAGEMENT CONSOLE
10
REMOTE MANAGEMENT SERVER
20
OBTAINS A LIST OF INFORMATION PROCESSING APPARATUSES
SENDS A LIST OF INFORMATION PROCESSING APPARATUSES
DECIDES INFORMATION PROCESSING APPARATUS
OBTAINS FIRMWARE INFORMATION
OBTAINS FIRMWARE INFORMATION FROM THE INFORMATION PROCESSING APPARATUS
SENDS FIRMWARE VERSION AND UPDATABLE FIRMWARE VERSION
DECIDES UPDATABLE FIRMWARE VERSION
DECIDES UPDATE FIRMWARE
REQUESTS EXECUTION OF FIRMWARE UPDATE
EXECUTES FIRMWARE UPDATE PROCESSING

FIG. 6

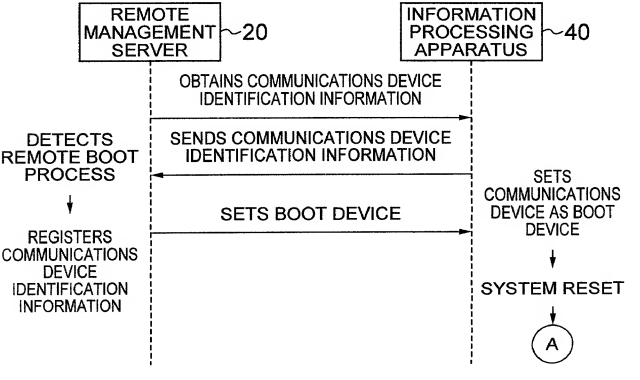

REMOTE MANAGEMENT SERVER
20
INFORMATION PROCESSING APPARATUS
40
OBTAINS COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION
DETECTS REMOTE BOOT PROCESS
SENDS COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION
SETS COMMUNICATIONS DEVICE AS BOOT DEVICE
SETS BOOT DEVICE
REGISTERS COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION
SYSTEM RESET
A

FIG. 7

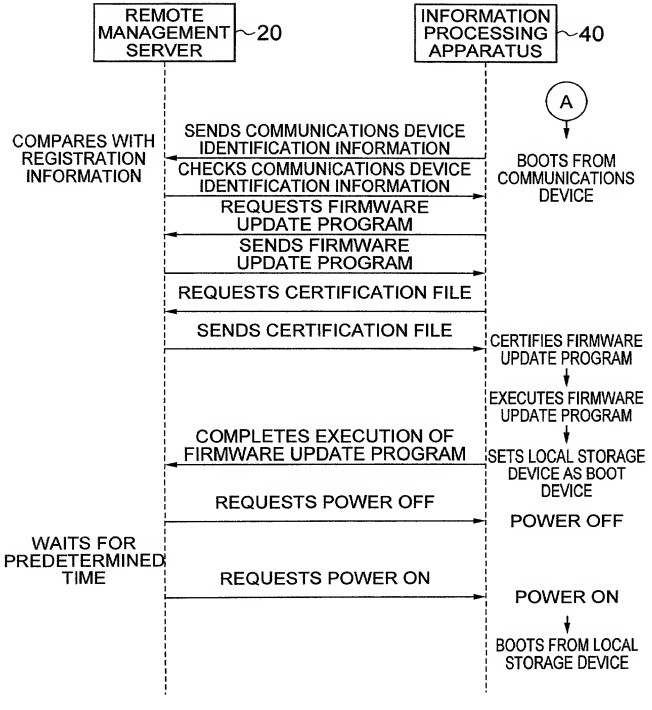
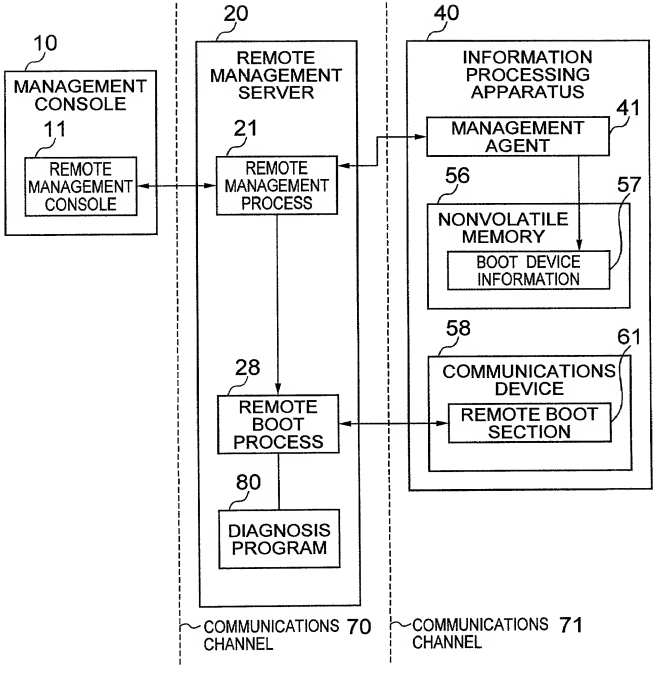

REMOTE MANAGEMENT SERVER
20
INFORMATION PROCESSING APPARATUS
40
A
COMPARES WITH REGISTRATION INFORMATION
SENDS COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION
CHECKS COMMUNICATIONS DEVICE IDENTIFICATION INFORMATION
BOOTS FROM COMMUNICATIONS DEVICE
REQUESTS FIRMWARE UPDATE PROGRAM
SENDS FIRMWARE UPDATE PROGRAM
REQUESTS CERTIFICATION FILE
SENDS CERTIFICATION FILE
CERTIFIES FIRMWARE UPDATE PROGRAM
EXECUTES FIRMWARE UPDATE PROGRAM
COMPLETES EXECUTION OF FIRMWARE UPDATE PROGRAM
SETS LOCAL STORAGE DEVICE AS BOOT DEVICE
REQUESTS POWER OFF
POWER OFF
WAITS FOR PREDETERMINED TIME
REQUESTS POWER ON
POWER ON
BOOTS FROM LOCAL STORAGE DEVICE

FIG. 8


10
MANAGEMENT CONSOLE
11
REMOTE MANAGEMENT CONSOLE
20
REMOTE MANAGEMENT SERVER
21
REMOTE MANAGEMENT PROCESS
28
REMOTE BOOT PROCESS
80
DIAGNOSIS PROGRAM
40
INFORMATION PROCESSING APPARATUS
41
MANAGEMENT AGENT
56
NONVOLATILE MEMORY
57
BOOT DEVICE INFORMATION
58
COMMUNICATIONS DEVICE
61
REMOTE BOOT SECTION
COMMUNICATIONS CHANNEL 70
COMMUNICATIONS CHANNEL 71